

# Completing the proof of “Generic quantum nonlocality”

Mariami Gachechiladze and Otfried Gühne

Naturwissenschaftlich-Technische Fakultät, Universität Siegen,  
Walter-Flex-Str. 3, 57068 Siegen, Germany

March 9, 2017

## Abstract

In a paper by Popescu and Rohrlich [Phys. Lett. A **166**, 293 (1992)] a proof has been presented showing that any pure entangled multiparticle quantum state violates some Bell inequality. We point out a gap in this proof, but we also give a construction to close this gap. It turns out that with some extra effort all the results from the aforementioned publication can be proven. Our construction shows how two-particle entanglement can be generated via performing local projections on a multiparticle state.

## 1 Introduction

The question which quantum states violate a Bell inequality and which not is of central importance for quantum information processing. In Ref. [1] it has been shown that any pure multiparticle quantum state violates a Bell inequality. The strategy for proving this statement was the following: First, one can show that for any entangled pure state on  $N$  particles one can find projective measurements on  $N - 2$  particles, such that for appropriate results of the measurements the remaining two particles are in an entangled pure state. Then, one can apply the known fact that any pure bipartite entangled state violates some Bell inequality [2].

In this note we point out a gap in the proof presented in Ref. [1]. The gap concerns the part where the projective measurements on  $N - 2$  particles are made. It turns out that a certain logical step does not follow from the previous statements and we give an explicit counterexample for a conclusion drawn at the critical point. Luckily it turns out, however, that with a significantly refined and extended argumentation the main statement can still be proven. Independently of the connection to Ref. [1] our results provide a constructive way how a two-particle entangled state can be generated from an  $N$ -particle state by performing local projections onto  $N - 2$  particles. This may be of interest for the theory of multiparticle entanglement.

This note is organized as follows. In Section 2 we discuss the proof from Ref. [1] and the problem with a Lemma used there. In Section 3 we present a detailed proof of the required statement for qubits. Finally, in Section 4 we discuss the higher-dimensional case as well as some other observations needed for the proof.

## 2 Discussion of the original argument

The gap concerns the proof of the Lemma on page 296 of Ref. [1]. This lemma states that:

*Let  $|\psi\rangle$  be an  $N$  system entangled state. For any two of the  $N$  systems, there exists a projection onto a direct product of state of the other  $N-2$  systems, that leaves the two systems in an entangled state.* In the following we show that while the Lemma is correct, there is a gap in its original proof. Doing so, in this section we will reformulate the proof in modern language in order to see where the problem is. For simplicity, we first consider only qubits.

The proof from Ref. [1] is a proof by contradiction, so it starts with assuming the opposite. So, orthogonal basis vectors  $|b_i\rangle \in \{|0\rangle, |1\rangle\}$  are considered for each qubit  $i$ , where the conclusion does not hold. That is,

$$\langle b_3|\langle b_4|\dots\langle b_N|\psi\rangle = |\alpha\rangle|\beta\rangle, \quad (1)$$

where the projections are carried out on the qubits  $3, \dots, N$  and the qubits one and two remain in the product state  $|\alpha\rangle|\beta\rangle$  for any possible choice of the  $\langle b_3|\langle b_4|\dots\langle b_N|$ . The  $\langle b_i|$  can take the values 0 or 1. So, the product vector will in general depend on this choice and it is appropriate to write this dependency as

$$|\alpha\rangle = |\alpha(b_3, \dots, b_N)\rangle \quad \text{and} \quad |\beta\rangle = |\beta(b_3, \dots, b_N)\rangle. \quad (2)$$

What happens if the value of  $b_3$  changes? The proof in Ref. [1] argues convincingly that then not *both* of the  $|\alpha\rangle$  and  $|\beta\rangle$  can change: If this were the case, a projection onto the superposition  $\langle c_3| = \langle b_3 = 0| + \langle b_3 = 1|$ , while keeping  $\langle b_4|\dots\langle b_N|$  constant projects the system on the first two qubits in an entangled state. So, we have either

$$|\alpha\rangle = |\alpha(\circ, b_4, \dots, b_N)\rangle \quad \text{or} \quad |\beta\rangle = |\beta(\circ, b_4, \dots, b_N)\rangle, \quad (3)$$

where the “ $\circ$ ” indicates that  $|\alpha\rangle$  or  $|\beta\rangle$  for the given values of  $b_4, \dots, b_N$  does not depend on  $b_3$ .

The original proof continues the argument as follows: *Repeating the argument for other subspaces, we conclude that ... each index  $[b_i]$  actually appears in either  $|\alpha\rangle$  or in  $|\beta\rangle$  but not in both.* This conclusion is unwarranted. The point is that for a given set of  $b_4, \dots, b_N$  one of the vectors (say,  $|\alpha\rangle$  for definiteness) does not depend on  $b_3$ , but for another choice of  $b_4, \dots, b_N$  the other vector  $|\beta\rangle$  may be independent on  $b_3$ , while  $|\alpha\rangle$  may depend on it. So, one cannot conclude that one of the vectors is *generally* independent.

The problem is best illustrated with a counterexample. Consider the four-qubit state

$$|\psi\rangle = \frac{1}{2}(|0000\rangle + |0101\rangle + |0110\rangle + |1111\rangle). \quad (4)$$

One can easily check that this is not a product state for any bipartition, so the state is genuine multiparticle entangled. Also, any projection into the computational basis on the particles three and four leaves the first two particles in a product state. We have for the dependencies:

$$|\alpha(00)\rangle = |0\rangle, \quad |\alpha(01)\rangle = |0\rangle, \quad |\alpha(10)\rangle = |0\rangle, \quad |\alpha(11)\rangle = |1\rangle, \quad (5)$$

and

$$|\beta(00)\rangle = |0\rangle, \quad |\beta(01)\rangle = |1\rangle, \quad |\beta(10)\rangle = |1\rangle, \quad |\beta(11)\rangle = |1\rangle, \quad (6)$$

so neither of these vectors does depend on a single index only.

Of course, if one chooses measurements in other directions on the qubits three and four, that is, one measures vectors like

$$|c_3\rangle = \cos(\gamma)|0\rangle + \sin(\gamma)|1\rangle \text{ and } |c_4\rangle = \cos(\delta)|0\rangle + \sin(\delta)|1\rangle, \quad (7)$$

then the remaining state on the qubits one and two is entangled. So the state  $|\psi\rangle$  is not a counterexample to the main statement of the Lemma, but it demonstrates that proof requires some extra work.

Finally, if one accepts the step that each index  $[b_i]$  occurs only in  $|\alpha\rangle$  or  $|\beta\rangle$ , but not in both, one can conclude as demonstrated in Ref. [1] that the original state has to factorize, so it is not entangled.

### 3 Completing the argument

The previous section demonstrated that the proof of the Lemma in Ref. [1] is missing some discussions in order to be complete. In this section we provide a way to add the missing part. We prove the following statement:

*Let  $\mathbf{b}' = (b_3, b_4, \dots, b_N)$  with  $b_i \in \{0, 1\}$  be the basis vectors which are used for the projection on the qubits  $3, \dots, N$  and denote the remaining product state on the first two qubits by  $|\alpha(\mathbf{b}')\rangle|\beta(\mathbf{b}')\rangle$ . Then,  $|\alpha(\cdot)\rangle$  depends only on some subset of the indices  $\mathbf{b}'$ , while  $|\beta(\cdot)\rangle$  depends on the complement subset. This statement implies the correctness of the Lemma in Ref. [1].*

The proof is done by assuming the opposite and reaching a contradiction. The opposite claim is that there exists an index  $i$  (without the loss of generality, we can take  $i = 3$ ) and two sets of values for the remaining indices

$$\mathbf{b} = b_4, b_5, \dots, b_N \quad \text{and} \quad \mathbf{B} = B_4, B_5, \dots, B_N, \quad (8)$$

such that

$$|\alpha(0, \mathbf{b})\rangle \neq |\alpha(1, \mathbf{b})\rangle \quad \text{and} \quad |\beta(0, \mathbf{B})\rangle \neq |\beta(1, \mathbf{B})\rangle, \quad (9)$$

meaning that both depend on  $b_3$ . Here,  $|\alpha(0, \mathbf{b})\rangle$  is a short-hand notation for  $|\alpha(b_3 = 0, \mathbf{b})\rangle$ . Also, the inequality symbol here and in the following indicates linear independence, i.e.,  $|\alpha(0, \mathbf{b})\rangle \neq \lambda |\alpha(1, \mathbf{b})\rangle$  for any  $\lambda \neq 0$ .

The vectors  $\mathbf{b}$  and  $\mathbf{B}$  differ in some entries, but in some entries they match. Without loss of generality, we can assume that they differ in the first  $k$  entries while the others are the same and equal to zero. More specifically, they can be taken of the form:

$$\begin{aligned} \mathbf{b} &= 0 \ 0 \ 0 \ \dots \ 0 \ 0 \ 0 \ \dots \ 0, \\ \mathbf{B} &= \underbrace{1 \ 1 \ 1 \ \dots \ 1}_k \ \underbrace{0 \ 0 \ \dots \ 0}_{N-k-3}. \end{aligned} \quad (10)$$

Then the proof proceeds via induction on  $k$ . The precise statement we want to prove for all  $k$  is the following: Let the vectors  $\mathbf{b}$  and  $\mathbf{B}$  differ by at most at  $k$  terms. Then, if  $|\alpha(0\mathbf{b})\rangle \neq |\alpha(1\mathbf{b})\rangle$ , the equality  $|\beta(0\mathbf{B})\rangle = |\beta(1\mathbf{B})\rangle$  must hold. The crucial point here is that on each induction step we need to use the already derived linear dependencies and independencies from all the previous induction steps, i.e. for all  $k' < k$ . We give the first ( $k = 0 \mapsto k = 1$ ) and the second ( $k = 1 \mapsto k = 2$ ) step of the induction explicitly, as this is needed in order to get the idea for the general case. This general case is discussed afterwards.

- (a) The base case: If  $k = 0$ , then  $\mathbf{b} = \mathbf{B}$  and the proof for this particular case is included in the discussion in Section 2 and in Ref. [1].
- (b)  $k = 0 \mapsto k = 1$  :  
 As  $|\alpha(\cdot)\rangle$  and  $|\beta(\cdot)\rangle$  depend on  $b_3$  and  $b_4$  only, we can suppress the other indices and we write  $|\alpha(00)\rangle, |\alpha(01)\rangle$ , etc. Using this notation the problem boils down to showing that

$$|\alpha(00)\rangle \neq |\alpha(10)\rangle \quad \text{and} \quad |\beta(01)\rangle \neq |\beta(11)\rangle \quad (11)$$

cannot happen simultaneously. We show that if this would be true, it would contradict the assumption that the state after projection is a product state.

From step (a) we already know that the statement is correct for  $k = 0$ , which means that if only one value changes, then only one of  $|\alpha(\cdot)\rangle$  and  $|\beta(\cdot)\rangle$  can change. We can use this in the following way: For  $x = 0$  or  $1$ , if  $|\alpha(0x)\rangle \neq |\alpha(1x)\rangle$ , it follows that  $|\beta(0x)\rangle = |\beta(1x)\rangle$ . Furthermore,  $|\alpha(x0)\rangle \neq |\alpha(x1)\rangle$  implies that  $|\beta(x0)\rangle = |\beta(x1)\rangle$ . And similarly, we can conclude equalities for the  $|\alpha(\cdot)\rangle$  from inequalities of the  $|\beta(\cdot)\rangle$ .

Assuming that the statement in Eq. (11) can be satisfied, we would like to reach a contradiction. From the conditions in Eq. (11) and our previous argumentation it follows that

$$|\alpha(01)\rangle = |\alpha(11)\rangle \quad \text{and} \quad |\beta(00)\rangle = |\beta(10)\rangle. \quad (12)$$

Now there are two cases to be considered and in both cases a contradiction is reached:

1. The case  $|\alpha(00)\rangle \neq |\alpha(01)\rangle$ :  
 Then from the result for  $k = 0$  an equality follows for the  $|\beta(\cdot)\rangle$ , namely  $|\beta(00)\rangle = |\beta(01)\rangle$ . This implies with Eqs. (12) and (11) that  $|\beta(10)\rangle \neq |\beta(11)\rangle$ . Consequently, we get that  $|\alpha(10)\rangle = |\alpha(11)\rangle$  and from Eq. (12) it follows that  $|\alpha(10)\rangle = |\alpha(01)\rangle$ .  
 To sum up all the relations for  $|\alpha(\cdot)\rangle$  and  $|\beta(\cdot)\rangle$ , we can write:

$$\begin{aligned} |\tilde{\alpha}\rangle &\equiv |\alpha(01)\rangle = |\alpha(10)\rangle = |\alpha(11)\rangle \neq |\alpha(00)\rangle, \\ |\tilde{\beta}\rangle &\equiv |\beta(00)\rangle = |\beta(01)\rangle = |\beta(10)\rangle \neq |\beta(11)\rangle. \end{aligned} \quad (13)$$

Now we project the total state  $|\psi\rangle$  onto  $|+\rangle_3|+\rangle_4$  on the qubits 3 and 4 and on  $|0\dots 0\rangle_{5\dots N}$  on the further qubits. Then, the remaining state on the first two qubits is:

$$|\psi\rangle_{12} = \sum_{i,j \in \{0,1\}} |\alpha(ij)\rangle |\beta(ij)\rangle = |\alpha(00)\rangle |\tilde{\beta}\rangle + |\tilde{\alpha}\rangle |\beta(11)\rangle + 2|\tilde{\alpha}\rangle |\tilde{\beta}\rangle. \quad (14)$$

Noting that  $|\alpha(00)\rangle \neq |\tilde{\alpha}\rangle$ , the state  $|\psi\rangle_{12}$  can only be a product state if

$$|\tilde{\beta}\rangle = 2|\tilde{\beta}\rangle + |\beta(11)\rangle, \quad (15)$$

which means that  $|\beta(11)\rangle = |\tilde{\beta}\rangle$  up to a factor. This is a contradiction.

2. The complement case  $|\alpha(00)\rangle = |\alpha(01)\rangle$ :

Then  $|\alpha(11)\rangle \neq |\alpha(10)\rangle$  and from Eqs. (12) and (11) we have

$$|\alpha\rangle \equiv |\alpha(00)\rangle = |\alpha(01)\rangle = |\alpha(11)\rangle \neq |\alpha(10)\rangle. \quad (16)$$

Furthermore, this implies that  $|\beta(10)\rangle = |\beta(11)\rangle$ . So,

$$|\beta\rangle = |\beta(00)\rangle = |\beta(10)\rangle = |\beta(11)\rangle \neq |\beta(01)\rangle. \quad (17)$$

The proof then proceeds as in the case 1.

(c)  $k = 1 \mapsto k = 2$  : As mentioned above, we also discuss this case in detail, as it reveals the main idea for the general case.

This case also starts by assuming the opposite, similar to Eq. (11):

$$|\alpha(000)\rangle \neq |\alpha(100)\rangle \quad \text{and} \quad |\beta(011)\rangle \neq |\beta(111)\rangle. \quad (18)$$

This means that if the **b** and **B** differ in two entries, we assume that it happens that  $|\alpha(\cdot)\rangle$  and  $|\beta(\cdot)\rangle$  both change under a flip of the first index. Eq. (18) states that  $|\alpha(x00)\rangle$  is not constant in  $x$ . Using the induction for  $k = 1$  it follows that  $|\beta(x00)\rangle$ ,  $|\beta(x01)\rangle$ , and  $|\beta(x10)\rangle$  are constant in  $x$ . Consequently, from Eq. (18) it follows that

$$|\alpha(001)\rangle = |\alpha(101)\rangle, \quad |\alpha(010)\rangle = |\alpha(110)\rangle, \quad (19)$$

$$|\beta(001)\rangle = |\beta(101)\rangle, \quad |\beta(010)\rangle = |\beta(110)\rangle. \quad (20)$$

Here we mention only the relations that we use at this stage of the proof.

Throughout the entire proof, to complete a particular induction step, it is crucial to deduce many combinations of specific indices and flips for which either  $|\alpha(\cdot)\rangle$  or  $|\beta(\cdot)\rangle$  changes. These type of linear independencies are of a particular interest because from them it follows that for the same combination of indices and flips  $|\beta(\cdot)\rangle$  or  $|\alpha(\cdot)\rangle$  cannot change, respectively. Therefore, for  $|\beta(\cdot)\rangle$  here we consider the following single-index flips:

$$|\beta(011)\rangle \xrightarrow{F_3} |\beta(010)\rangle \xrightarrow{F_1} |\beta(110)\rangle \xrightarrow{F_3} |\beta(111)\rangle, \quad (21)$$

where  $F_i$  denotes a flip of the value of the  $i$ -th index. Here the first and last term are linearly independent as assumed in Eq. (18), but the second and third are equal according to Eq. (20). So, since  $|\beta(\cdot)\rangle$  changes from the first to the last term, it has to change either in the first step or the last one.<sup>1</sup> If  $|\beta(\cdot)\rangle$  changes in the first step,  $|\beta(01x)\rangle$  is not constant, implying that  $|\alpha(00x)\rangle$ ,  $|\alpha(01x)\rangle$ , and  $|\alpha(11x)\rangle$  are constant in  $x$ . In the other case, if  $|\beta(\cdot)\rangle$  changes in the third step,  $|\beta(11x)\rangle$  is not constant, implying that  $|\alpha(01x)\rangle$ ,  $|\alpha(10x)\rangle$ , and  $|\alpha(11x)\rangle$  are constant in  $x$ .

This implies that in any case,  $|\alpha(01x)\rangle$  and  $|\alpha(11x)\rangle$  have to be constant. So, we have:

$$|\alpha(011)\rangle = |\alpha(010)\rangle \quad \text{and} \quad |\alpha(111)\rangle = |\alpha(110)\rangle. \quad (22)$$

---

<sup>1</sup>Also both can change, but there is no need to consider this separately as this is the simpler case: It includes the constraints from the both cases together. In fact, if both change, one even more directly see that this implies  $|\alpha(000)\rangle = |\alpha(100)\rangle$  and a contradiction.

For the future discussion it is useful to summarize this finding by stating that a flip of the third index ( $F_3$ ) cannot change  $|\alpha(\cdot)\rangle$ , unless the second index is zero.

The same argument can be applied to the different sequence:

$$|\beta(011)\rangle \xrightarrow{F_2} |\beta(001)\rangle \xrightarrow{F_1} |\beta(101)\rangle \xrightarrow{F_2} |\beta(111)\rangle. \quad (23)$$

Here again first and last term differ and the middle terms are equal. Similar as above, this implies that the flips ( $1F1$ ) and ( $0F1$ ) cannot change  $|\alpha(\cdot)\rangle$ , i.e.

$$|\alpha(101)\rangle = |\alpha(111)\rangle \quad \text{and} \quad |\alpha(001)\rangle = |\alpha(011)\rangle. \quad (24)$$

Again, we can state that  $F_2$  cannot change  $|\alpha(\cdot)\rangle$ , unless the third index is zero.

From these observations it follows that:

$$|\alpha(001)\rangle \xrightarrow{F_2} |\alpha(011)\rangle \xrightarrow{F_3} |\alpha(010)\rangle \xrightarrow{\text{Eq.19}} |\alpha(110)\rangle \xrightarrow{F_3} |\alpha(111)\rangle \xrightarrow{F_2} |\alpha(101)\rangle. \quad (25)$$

This means that  $|\alpha(\cdot)\rangle$  can take only three values, two from the Eq. (18) and one from the Eq. (25).

Similarly, we can repeat the steps for the other side. Here, it turns out that  $|\beta(\cdot)\rangle$  cannot change under the flip  $F_3$  (resp.,  $F_2$ ) unless the second (resp., third) index is one. It follows that  $|\beta(\cdot)\rangle$  can take only three values as we have:

$$|\beta(010)\rangle \xrightarrow{F_2} |\beta(000)\rangle \xrightarrow{F_3} |\beta(001)\rangle \xrightarrow{\text{Eq.20}} |\beta(101)\rangle \xrightarrow{F_3} |\beta(100)\rangle \xrightarrow{F_2} |\beta(110)\rangle. \quad (26)$$

There are again two cases to consider and each of them leads to a contradiction:

1. The case  $|\alpha(000)\rangle \neq |\alpha(001)\rangle$ :

Then from the induction requirement we have  $|\beta(011)\rangle = |\beta(010)\rangle$ , which implies that  $|\beta(\cdot)\rangle$  can take only two values. Furthermore, from  $|\beta(111)\rangle \neq |\beta(110)\rangle$  it follows that  $|\alpha(100)\rangle = |\alpha(101)\rangle$ , which itself means that  $|\alpha(\cdot)\rangle$  can take only two values.

Then, we proceed as in the part (b) above. We project onto the product state  $|+\rangle_3|+\rangle_4|+\rangle_5|0\rangle^{\otimes N-5}$  and we cannot get a product state unless  $|\beta(\cdot)\rangle$  is constant. This contradicts the initial assumption in Eq. (18).

2. The case  $|\alpha(000)\rangle = |\alpha(001)\rangle$ :

This means that  $|\alpha(\cdot)\rangle$  can only take two values. Besides,  $|\alpha(101)\rangle \neq |\alpha(100)\rangle$  implies that  $|\beta(111)\rangle = |\beta(110)\rangle$ . So,  $|\beta(\cdot)\rangle$  can take only two values. Similarly to the previous case, the projection onto the state  $|+\rangle_3|+\rangle_4|+\rangle_5|0\rangle^{\otimes N-5}$  leads to the contradiction.

- (d) The general case,  $k-1 \mapsto k$ :

As before, we assume that the following inequalities happen simultaneously:

$$|\alpha(\underbrace{0 \ 00 \dots 0}_k)\rangle \neq |\alpha(\underbrace{1 \ 00 \dots 0}_k)\rangle \quad \text{and} \quad |\beta(\underbrace{0 \ 11 \dots 1}_k)\rangle \neq |\beta(\underbrace{1 \ 11 \dots 1}_k)\rangle. \quad (27)$$

Similar to the previous cases, there are many equalities coming from the previous induction steps. Namely, we know already that a flip of the value of one index cannot both change  $|\alpha(\cdot)\rangle$  and  $|\beta(\cdot)\rangle$ , if the remaining indices differ at  $k - 1$  or less positions. This is the induction hypothesis that has to be used.

Now the following sequence of single index flips is considered:

$$|\beta(01 \dots 11)\rangle \xrightarrow{F_{k+1}} |\beta(01 \dots 10)\rangle \xrightarrow{F_1} |\beta(11 \dots 10)\rangle \xrightarrow{F_{k+1}} |\beta(11 \dots 1)\rangle. \quad (28)$$

Here the first and the last terms differ again according to the assumption, but the middle two entries are equal (this comes from the induction hypothesis mentioned above). So,  $|\beta(\cdot)\rangle$  must change in the first or third step.

This implies that  $|\alpha(\cdot)\rangle$  is not allowed to change under a flip  $F_{k+1}$ , unless the values of the indices  $2, \dots, k$  are all zero. To see this, let us assume that they are not all zeros. This means that there is at least one digit in common with  $1 \dots 1$  on the indices  $2, \dots, k$ .

On the one hand, then they differ only in  $k - 1$  or less digits from the string  $01 \dots 1$  on the indices  $1, \dots, k$ . By the induction hypothesis we can conclude that  $|\alpha(\cdot)\rangle$  is not allowed to change if  $|\beta(\cdot)\rangle$  changes in the first step of the sequence.

On the other hand, they also differ in less or equal  $k - 1$  digits from the string  $11 \dots 1$  on the indices  $1, \dots, k$ , so  $|\alpha(\cdot)\rangle$  is not allowed to change if  $|\beta(\cdot)\rangle$  changes in the third step of the sequence. Since  $|\beta(\cdot)\rangle$  has to change in the first or third step,  $|\alpha(\cdot)\rangle$  can not change under a flip  $F_{k+1}$ , unless the values of the indices  $2, \dots, k$  are all zero.

By considering a similar sequence of flips,  $F_j \circ F_1 \circ F_j$  with  $j \in \{2, \dots, k\}$ , we can see that  $|\alpha(\cdot)\rangle$  cannot change under a flip  $F_j$ , unless all of the indices  $i \in \{2, \dots, k + 1\}$  with  $i \neq j$  are zero.

In addition, from the condition on  $|\beta(\cdot)\rangle$  in Eq. (27) and the induction hypothesis it follows that

$$|\alpha(100 \dots 01)\rangle = |\alpha(00 \dots 01)\rangle. \quad (29)$$

In combination with the invariance of  $|\alpha(\cdot)\rangle$  under the flips  $F_j$  mentioned above this implies that the terms in Eq. (29) are also equal to all other  $|\alpha(\cdot)\rangle$  except to the two  $|\alpha(\cdot)\rangle$  given in Eq. (27). Namely, any  $|\alpha(\cdot)\rangle$  where not all indices  $2, \dots, k + 1$  are zero can be brought to  $|\alpha(100 \dots 01)\rangle$  or  $|\alpha(00 \dots 01)\rangle$  by flips  $F_j$  on the indices  $j \in \{2, \dots, k + 1\}$ .

Therefore,  $|\alpha(\cdot)\rangle$  can take only three values: two for the assumption in Eq. (27) and one for the rest of the  $(2^{k+1} - 2)$  terms. Exactly the same argument holds for  $|\beta(\cdot)\rangle$ . Consequently, we again consider two cases, reduce the three values to two for both  $|\alpha(\cdot)\rangle$  and  $|\beta(\cdot)\rangle$ , and upon projecting on the product state, we reach the contradiction that  $|\beta(\cdot)\rangle$  can only have one value.

This ends the proof of the statement at the beginning.

In the following section, however, we need to consider the extension to the  $d$ -dimensional case. Besides, we need to be cautious that the projections in the

computational basis always give non-vanishing coefficients. Below we demonstrate that this condition can always be achieved and it does not impose any limitations on the Lemma.

## 4 Additional Remarks

### 4.1 Generalization to the $d$ -dimensional case

So far, we have discussed only multi-qubit systems and the question arises, whether the results can be extended to higher dimensional systems. There are two ways to deal with this issue. First, one can extend the discussion of Section 3 also to the higher dimensions. The point is that in Section 3 the core conditions were always stating that certain indices are equal or not equal. This, of course, can be formulated also for non-binary indices. A second and more elegant way, however, makes use of the fact that any  $N$ -qudit entangled pure state can be projected by local means on an entangled  $N$ -qubit entangled state. This can be achieved by the following procedure:

Let  $|\psi\rangle$  be a  $d \times d \times \dots \times d$  entangled state, where  $d$  is the dimension of the Hilbert space associated with each system. We start by considering the first subsystem and write down the Schmidt decomposition with respect to the split  $1|2, 3, 4, \dots, N$ :

$$|\psi\rangle = \sum_{i=1}^d s_i |i\rangle_1 |i\rangle_{2,3,4,\dots,N}. \quad (30)$$

Then, we proceed as follows:

1. If  $|\psi\rangle$  is separable with respect to the  $1|2, 3, 4, \dots, N$  partition, the sum consists only of one term and we do nothing. Note that effectively the whole state lives on a one-dimensional subspace on Alice's side, so one can view it as a  $1 \times d \times \dots \times d$  state.
2. If  $|\psi\rangle$  is entangled with respect to the  $1|2, 3, 4, \dots, N$  partition, we project locally for Alice onto the two first Schmidt vectors, resulting in the truncated sum:

$$|\psi'\rangle = \sum_{i=1,2} s'_i |i\rangle_1 |i\rangle_{2,3,4,\dots,N}. \quad (31)$$

This state is still entangled with respect to the  $1|2, 3, 4, \dots, N$  partition and it is a  $2 \times d \times \dots \times d$  state.

Now, we go on and do the same procedure iteratively for particle 2, then particle 3, etc., until we arrive at the last party  $N$ . At the end we have a state living in a  $2 \times 2 \times \dots \times 2$ -dimensional Hilbert space. If the original state was entangled, then the state  $|\psi'\rangle$  is also entangled: when going through the parties, there will be some party, say  $j$ , where the last projection according to point (2) above is made. So the final state will be entangled with respect to the  $j|\mathbf{rest}$  partition (where  $\mathbf{rest}$  denotes all the remaining parties) and it is not a fully separable state. Note that the projection on  $j$  may change the separability properties of the  $1|\mathbf{rest}$  partition, and this partition may become separable. However, at least one entangled partition remains, and as discussed above, this is sufficient to show that the state is not a fully separable state.



So any entangled  $d \times d \times \cdots \times d$  pure state can be projected locally onto a pure entangled  $N$ -qubit state and for qubit states we already repaired the proof.

## 4.2 The question of non-vanishing coefficients

A further point worth to discuss is the question whether the state  $|\psi\rangle$  considered in the proof has maybe vanishing coefficients in the basis where the projections are made. In fact, the careful reader may have noticed that for the theorem and the proof above to work, it is required all possible projections in the computational basis, especially the states  $|\alpha(\cdot)\rangle$  and  $|\beta(\cdot)\rangle$  are non-zero. This might not be fulfilled for a given basis.

Of course, for a random choice of the product basis this will be in general fulfilled. More constructively, one can ask whether there is a set of local unitaries that, when applied to any initial state  $|\psi\rangle$  in the computational basis, give *with certainty* some states where all the coefficients are non-vanishing. Interestingly, this question was brought up as one of the “ten most annoying questions in quantum computing” [3] with the local unitaries being the Hadamard gates and the solution was given in Ref. [4]. We now recall this result in the following lemma with the notation  $\sigma_x$  and  $\sigma_z$  being the Pauli- $X$  and Pauli- $Z$  matrices, respectively.

**Lemma [4].** *Given an  $N$ -qubit pure state, there is always a way to apply Hadamard gates to some subset of the qubits to make all  $2^N$  computational basis components having non-zero amplitudes. In other words, if one considers the  $2^N$  product bases defined by the eigenstates of the observables  $\sigma_{k_1}^{(1)} \otimes \cdots \otimes \sigma_{k_N}^{(N)}$  with  $\sigma_k^{(j)} \in \{\sigma_x, \sigma_z\}$ , then any state  $|\psi\rangle$  has non-vanishing coefficients in at least one of these bases.*

This Lemma guarantees that a suitable basis can be found in a constructive manner.  $\square$

## Acknowledgments

We thank Carmen Constatin and Matty Hoban for discussions. We especially thank Sandu Popescu, Daniel Rohrlich, and Paul Skrzypczyk for comments on the manuscript, they agree on the points raised here. This work was supported by the DFG, the ERC (Consolidator Grant 683107/TempoQ) and the FQXi Fund (Silicon Valley Community Foundation).

## References

- [1] S. Popescu and D. Rohrlich, Phys. Lett. A **166**, 293 (1992).
- [2] N. Gisin and A. Peres, Phys. Lett. A **162**, 15 (1992).
- [3] S. Aaronson, *The ten most annoying questions in quantum computing* (2006), available at [www.scottaaronson.com/blog/?p=112](http://www.scottaaronson.com/blog/?p=112).
- [4] A. Montanaro and D. J. Shepherd, *Hadamard gates and amplitudes of computational basis states* (2006), available at [www.scottaaronson.com/hadamard.pdf](http://www.scottaaronson.com/hadamard.pdf).